Security & Confidentiality in ImmPact

Security implementation in ImmPact combines a high level of Web-based security with additional application-specific data access rules. This multi-tiered approach is designed to protect from unauthorized use the potentially sensitive information which ImmPact retains on patients and their immunization status.

World Wide Web Security

The approach to securing information on the World Wide Web differs depending on the need to allow or prevent individual access to specific pieces of data. The three levels of security outlined here are the most common.

Unsecured Access

A majority of the information published on the World Wide Web is readily accessible by any individual with a Web browser. This includes information web sites featuring companies and promoting their products, sites containing news and sports, and sites containing non-classified, generally available data.

User Authentication

Web sites that contain either personalized or sensitive data usually require user authentication at the beginning of a session. A common form of authentication is the use of a username and password which are unique to the individual. Knowing a password indicates that a user is who he or she says they are. There is a chance, however, that someone "listening" in on the computer network can decipher a username/password combination and pretend to be that user at a later time.

User Authentication and Secured Sockets

To prevent the stealing of authentication parameters by network hackers, the use of a username and password is often combined with a secure communication mechanism such as the Secured Sockets Layer (SLL). SSL is a communication protocol that encrypts the information packets which travel on the network between the Web browser and the Web server. SSL uses government-approved 128-bit encryption algorithm and is nearly impossible to break.

ImmPact Application Security

In addition to Web specific mechanisms outlined above, ImmPact uses its own security design to control the access of information. Users are given access to ImmPact and assigned a username and password through a centrally controlled process. In addition to the username and password, the user is associated with a specific health care provider and is assigned to a specific role. Role restrictions can be made on access to data fields or parts of ImmPact so that only the parts the user is allowed to see are visible. (For example, a clerk who only orders vaccine will be allowed to see only the screens for ordering vaccines and can never access patient records.)

The information in the ImmPact system is made available based on a need-to-know/need-to-access model. The ImmPact application logic defines access to an individual record as a function of the user's secured username/password, their relationship to the provider, their assigned role, and the patient's relationship to the provider. This combination ensures that only those individuals who truly need to access the information or functions are given access.

Access Controls

ImmPact
Security & Confidentiality in ImmPact

Last Revised: 02/29/2000

- Access to ImmPact will be limited to those providers that have signed a confidentiality agreement with the Department of Health and Human Services.
- The user will be linked to a specific provider location that has been authenticated.
- Access privileges to individual records is limited by the need to know. Three levels of providers have been defined to control data access:

  Primary Providers
  These providers have agreed to assume responsibility for the immunization status of the patient. These providers will have access and actively maintain patient demographic and immunization information.
  Secondary Providers
  These providers are in practice or associated with the primary provider and may have access to patient demographic and immunization information, but do not actively maintain it and do not assume responsibility for the patient's immunization status.
  Ancillary Providers
  These providers see the patient on a one-time or emergency basis. These providers must be able to provide enough identifying information on the patient to ensure the patient viewed on the screen is the patient in the office. They cannot "browse" records, but must be able to match the record exactly. This provider can see the immunization record and add any immunizations given, but they cannot read patient demographic information or make any changes to that record.

- Each user is assigned a role. This role specifically grants privileges to information that can be accessed and/or changed by the user. Users will not have any access to screens or data that they are not authorized to use.
- Each user has their own user account and password to access the system.
- Audit trails will identify all attempts to access the system and the individual record will be stamped with the date, time, and user name when the record changes or additions are made.

Release of Information

- Individuals will be informed when their provider is participating in ImmPact. They may choose to not participate at that point by completing a form for their provider. At any point, the patient may choose to have their information deleted by requesting it of their health care provider or by submitting a request to the New Hampshire Immunization Program. (Rules are currently being developed to address how this procedure will occur.)
- Individuals may see their information in ImmPact by requesting a copy of their record from their health care provider according to their provider's medical record policies. They may also make a request to the New Hampshire Immunization Program. (Rules are currently being developed to address how this procedure will occur.)